

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

Facebook account with username Jason Williams, UID
100015332224949, username Jason Williams, UID
100002038949110, and username John Evans, UID
100001254606978, more fully described in Attachment A

Case No. 17-947M (WJ)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

Facebook account with username Jason Williams, UID 100015332224949, username Jason Williams, UID 100002038949110, and username John Evans, UID 100001254606978, more fully described in Attachment A

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of:

Title 18, United States Code, Sections 1951 and 2 (Hobbs Act Robbery), and Title 18 United States Code, Sections 924(c) (use of a firearm during a crime of violence)

The application is based on these facts: See attached affidavit.

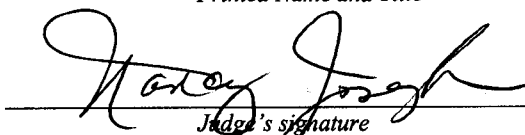
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


 Applicant's signature

Erin Lucker, Special Agent FBI
 Printed Name and Title

Sworn to before me and signed in my presence:

Date: October 20, 2017


 Judge's signature

City and State: Milwaukee, Wisconsin Case 17-17317-mj-00947-NJ Filed 12/11/17 Nancy Joseph, U.S. Magistrate Judge 1
 Printed Name and Title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR SEARCH WARRANTS

I, Erin Lucker, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain Facebook user IDs that are stored at premises owned, maintained, controlled, or operated by Facebook Inc. ("Facebook"), a social networking company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the user IDs as described in Attachment A.

2. I am a Special Agent of the Federal Bureau of Investigation (FBI) and have been so employed since November 2016. I am currently assigned to the Milwaukee Office of the FBI. During my career in law enforcement, I have participated in violent crime investigations. I am currently assigned to the FBI Milwaukee Violent Crimes Task Force, which involves investigations of violent crimes, including kidnappings, extortions, murder for hire, and bank and armored car robberies. I have gained experience in the conduct of such investigations through previous case investigations, formal training, and in consultation with law enforcement partners in local, state, and federal law enforcement agencies.

3. I have participated in many violent crime investigations that involved the seizure of computers, cellular phones, cameras, and other digital storage devices, and the subsequent analysis of electronic data stored within these computers, cellular phones, cameras, and other

digital storage devices. On many occasions, this electronic data has provided evidence of the crimes being investigated and corroborated information already known or suspected by law enforcement. Based on my experience and training, I know that robbers often use electronic equipment, such as computers, laptop computers, and cellular telephones to facilitate their criminal enterprise. I further know that robbers sometimes use Facebook and "Facebook Messenger" to discuss criminal activity.

4. The facts in this affidavit come from my personal observations, my training and experience, information obtained from witnesses, and information obtained from other agents during the course of their official duties, all of whom I believe to be truthful and reliable. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based upon my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 1951(a) (Hobbs Act Robbery) and Title 18, United States Code, Section 924(c) (Use of Firearm during Crime of Violence) have been committed by Lamont D. Harris, John T. Evans, and Jason S. Williams. There is also probable cause to search the information described in Attachment A for evidence of these as described in Attachment B.

PROBABLE CAUSE

6. On April 24, 2017, at approximately 7:52 p.m., two unidentified black males robbed the Metro PCS located at 5606 75th St., Kenosha, WI. The robbers entered the store, and asked the store employee, K.N., about phone chargers. While K.N. was showing the taller suspect (Suspect 1) the charger, Suspect 1 pulled a black handgun from his right side. Suspect 1 held the gun to K.N.'s head and told K.N. to give him all of the money from the register. While Suspect 1

took money from the register, the shorter suspect (Suspect 2) duct taped K.N.'s hands behind his back and put duct tape over his mouth. Suspect 2 then put phones from the store in a white bag. Suspect 2 took K.N.'s personal phone, but then gave it back to K.N. The robbers stole \$100, 47 phones, and 19 SIM cards. After the robbers left, K.N. broke free from the duct tape and called police. No video surveillance was recovered because the store had only been open for two days and security cameras had not been installed.

7. On April 27, 2017, at approximately 6:55 p.m., two unidentified black males robbed the Spring Mobile AT&T cell phone store located at 7115 Durand Ave #1, Mount Pleasant, WI. The two robbers entered the cell phone store and asked the store employee, K.N., to look at headphones. As K.N. was bending over to grab some headphones, the taller suspect (Suspect 1) stated, "This is a stick up, get into the back." K.N. turned around and saw Suspect 1 pointing a black handgun at his chest. Suspect 1 stated, "Work with me, don't be a hero. I don't want to see any blood." The suspects asked K.N. where the safe was located. The shorter suspect (Suspect 2) then told K.N. to put his hands behind his back. Suspect 2 duct taped K.N.'s hands behind his back and his two legs around the ankles. K.N. could hear the suspects taking cell phones out of the safe. In addition to stealing 53 cell phones in the safe, the suspects also stole K.N.'s cell phone and wallet.

8. After the suspects fled, K.N. broke free of the duct tape and called the police. During a search of the surrounding areas, police found a split open black garbage bag and 24 new cell phones in the Batteries Plus parking lot. The police also located K.N.'s cell phone near the black garbage bag and cell phones.

9. Several fingerprints were recovered from the 24 cell phones, duct tape, and garbage bag. The Wisconsin Crime Lab located fingerprints belonging to Lamont Deon HARRIS on the

duct tape and on one of the recovered iPhones. In addition, the Wisconsin Crime Lab located fingerprints belonging to Jason S. Williams on one of the recovered iPhone boxes.

10. Still photographs obtained from the surveillance at the Spring Mobile AT&T during the time of the robbery depict the two individuals who robbed K.N. One robber was wearing a hat, but neither robber wore masks covering their faces. Law enforcement showed the still photographs from the Spring Mobile AT&T robbery to the store employee of Metro PCS, who was robbed at gunpoint on April 24, 2017. The Metro PCS store employee recognized the two men as the individuals who robbed him on April 24, 2017.

11. A witness interviewed after the April 27, 2017 robbery indicated seeing a male running through a parking lot carrying a garbage bag, which broke and caused cell phone boxes to spill all over the ground. This witness observed the male throw the white cell phone boxes into the trunk of a white car, which was observed in the lot. A white sedan was observed on security cameras located near the robbery location as well as on squad video. Law enforcement responding to the robbery captured an image and license plate of a four-door white Chevrolet Malibu bearing WI registration 999XGD, which is registered to Eunice Jones at 93XX Florence Drive in Sturtevant, Wisconsin. Law enforcement has further determined that John Evans also resides at 93XX Florence Drive in Sturtevant, Wisconsin.

12. Based on the similarity of the above-described robberies and the Metro PCS victim's identification of the robbers as detailed in Paragraph 10, on May 15, 2017, United States Magistrate Judge William E. Duffin ordered certain wireless service providers to disclose records and information associated with cellular telephone towers that provided cell service to each of the robbery locations at and around the time of the above-described robberies.

13. Based on the records and information obtained from the service providers that provided cell service to each of the robbery locations, law enforcement officials have determined that the phone numbers 224-237-4678 and 262-237-3724 were in contact with one another during and around the time of both robberies. In other words, the individuals using these numbers make phone contact with one another during and around the time of the robbery of PCS Metro in Kenosha, Wisconsin and during and around the time of the robbery of Spring Mobile AT&T in Mount Pleasant, Wisconsin.

14. Specifically, on April 27, 2017 at 6:53:41 p.m., Harris, using phone number 224-237-4678, places a call to Evans at 262-237-3724. In addition, 224-237-4678 makes approximately nine calls to 262-237-3724 over the following five minutes (6:53:41 p.m. to 6:58:11 p.m.).

15. On April 24, 2017, 224-237-4678 makes an outgoing call to 262-237-3724 at 7:51:03 p.m. As previously stated, the robbery of Metro PCS occurred around 7:52 p.m. on April 24, 2017.

16. Law enforcement believes Lamont Harris was operating 224-237-4678 because on April 27, 2017 surveillance video showed Harris using a cell phone at 6:53:38 p.m. central time, which matches an outgoing call on a cell tower near Spring Mobile AT&T at 6:53:41 p.m. Furthermore, Lamont Harris was arrested by the Greenfield Police Department on August 6, 2017, and he provided to law enforcement the number 224-237-4678 as his own at this time.

17. Law enforcement believes Evans was operating 262-237-3724 because this number belongs to Evans in various public and law enforcement databases.

18. On August 25, 2017, Magistrate Judge William E. Duffin ordered AT&T to provide information about the location of 224-237-4678. On October 10, 2017, Magistrate Judge William

E. Duffin ordered an extension to AT&T regarding the location of 224-237-4678. On October 11, 2017, law enforcement officers conducted surveillance in the area of Winthrop Harbor, Illinois, where telephone number 224-237-4678 was located. Law enforcement officers made contact with Harris at the Abode Motel, 1128 Sheridan Road, Room 2, Winthrop Harbor, Illinois. Harris was arrested pursuant to a warrant issued by Magistrate Judge William E. Duffin on August 25, 2017.

19. On October 8, 2017, law enforcement in Zion, Illinois viewed surveillance stills from the armed robbery of Spring Mobile AT&T, 7115 Durand Ave #1, Mount Pleasant, Wisconsin, which occurred on April 27, 2017. Law enforcement identified one of the subjects as Jason S. Williams, indicating police had contact with Williams in June 2017 after receiving a complaint regarding Williams.

20. A comparison of the robbers, who were not masked, depicted in the surveillance video from the April 27, 2017, robbery of Spring Mobile AT&T with a driver's license identification photograph of Williams reveals substantial similarity between the robber pointing the gun and Williams.

21. A search of Facebook revealed two pages associated with Williams; the pages list the name "Jason Williams," with Facebook ID numbers 100015332224949 and 100002038949110. Publicly viewable photographs on the Facebook pages of "Jason Williams" were compared to known photographs and they were determined to be the same individual. Telephone number 224-413-4799 is also associated with "Jason Williams" Facebook ID 100015332224949. Based on the cell tower information provided by the service providers, telephone number 224-413-4799 was in the area of Metro PCS, 5606 75th St., Kenosha, Wisconsin on April 24, 2017 at the time of the robbery.

22. A search of Facebook revealed one page associated with Evans; the page lists the name "John Evans," with Facebook ID 100001254606978. Publicly viewable photographs on the Facebook page of "John Evans" were compared to known photographs and they were determined to be the same individual. Telephone number 262-237-3724, known to be used by Evans, is associated to the Facebook page "John Evans."

FACEBOOK INFORMATION

23. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

24. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers (for password retrieval), physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

25. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account

includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

26. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

27. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

28. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link

to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

29. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a Chat feature that allows users to send and receive instant messages through Facebook. These chat communications are stored in the chat history for the account. Facebook also has a Video Calling feature, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

30. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

31. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

32. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

33. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through

the account, such as “liking” a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user’s Facebook page.

34. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs (“blogs”), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

35. The Facebook Gifts feature allows users to send virtual “gifts” to their friends that appear as icons on the recipient’s profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other “pokes,” which are free and simply result in a notification to the recipient that he or she has been “poked” by the sender.

36. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

37. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications (“apps”) on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user’s access or use of that application may appear on the user’s profile page.

38. Some Facebook pages are affiliated with groups of users, rather than one individual user. Membership in the group is monitored and regulated by the administrator or head of the group, who can invite new members and reject or accept requests by users to enter. Facebook can identify all users who are currently registered to a particular group and can identify the administrator and/or creator of the group. Facebook uses the term “Group Contact Info” to describe the contact information for the group’s creator and/or administrator, as well as a PDF of the current status of the group profile page.

39. Facebook uses the term “Neoprint” to describe an expanded view of a given user profile. The “Neoprint” for a given user can include the following information from the user’s profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends’ Facebook user identification numbers; groups and networks of which the user is a member, including the groups’ Facebook group identification numbers; future and past event postings; rejected “Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Facebook applications.

40. Facebook also retains Internet Protocol (“IP”) logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user’s IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

41. Social networking providers like Facebook typically retain additional information about their users’ accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well as records of any actions taken by the provider or user as a result of the communications.

42. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user’s “Neoprint,” IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to “tag” their location in posts and Facebook “friends” to locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner’s state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner’s motive and intent to commit a crime (e.g.,

information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

43. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

44. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require Facebook to disclose the government copies of the records and other information (including contact of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B. Based on the facts contained within this affidavit, I believe that probable cause exists to search the devices, which are more particularly described in Attachment A for evidence of armed robbery.

CONCLUSION

45. Based upon the foregoing, I request that the Court issue the proposed search warrant.

46. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

47. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the following Facebook usernames and user IDs, which are stored at premises owned, maintained, controlled, or operated by Facebook Inc., a company headquartered in Menlo Park, California.

FACEBOOK NAME	FACEBOOK IDENTIFICATION (UID)
Jason Williams	100015332224949
Jason Williams	100002038949110
John Evans	100001254606978

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Facebook

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook Inc. ("Facebook"), including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each user ID listed in Attachment A:

- a. All contact and personal identifying information, including the full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers of Facebook Username: Jason Williams, Facebook User ID 100015332224949; Facebook Username: Jason Williams, Facebook User ID 100002038949110; and Facebook Username: John Evans, Facebook User ID 100001254606978.
- b. All activity logs for the account and all other documents showing the user's posts and other Facebook activities;
- c. All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them;
- d. All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which

- the user is a member, including the groups' Facebook group identification numbers;
future and past event postings; rejected "Friend" requests; comments; gifts; pokes;
tags; and information about the user's access and use of Facebook applications;
- e. All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;
 - f. All "check ins" and other location information;
 - g. All IP logs, including all records of the IP addresses that logged into the account;
 - h. All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked;"
 - i. All information about the Facebook pages that the account is or was a "fan" of;
 - j. All past and present lists of friends created by the account;
 - k. All records of Facebook searches performed by the account;
 - l. All information about the user's access and use of Facebook Marketplace;
 - m. The types of service utilized by the user;
 - n. The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
 - o. All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

- p. All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 18 U.S.C. 1951 (Hobbs Act Robbery) and 18 U.S.C. 924(c) (Use of Firearm During a Crime of Violence), since January 1, 2017, including, for each user ID identified on Attachment A, information pertaining to the following matters:

- a. The relevant offense conduct, any preparatory steps taken in furtherance of the scheme, communications between Lamont Harris, Jason Williams, John Evans, and others related to the relevant offense conduct of robbery;
- b. Evidence indicating how and when the Facebook account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook account owner;
- c. Evidence indicating the Facebook account owner's state of mind as it relates to the crime under investigation;
- d. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);
- e. The identity of the person(s) who communicated with the user ID about matters relating to relevant offense conduct of robbery, including records that help reveal their whereabouts.